

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HECTOR FABIAN RODRIGUEZ ALZATE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
IBAGUÉ
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HECTOR FABIAN RODRIGUEZ ALZATE

Diplomado de opción de grado presentado para optar el título de INGENIERO EN
TELECOMUNICACIONES

DIRECTOR
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
IBAGUÉ
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

IBAGUÉ, 22 de mayo de 2020

CONTENIDO

	Pág.
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN.....	8
ABSTRACT.....	8
INTRODUCCIÓN	9
DESARROLLO DE LA GUIA	10
Escenario 1.	10
Escenario 2	18
CONCLUSIONES	35
REFERENCIAS BIBLIOGRÁFICAS.....	36

LISTA DE TABLAS

	Pág.
Tabla 1. Direccionamiento escenario 1	11
Tabla 2. Asociacion de los puertos a las vlan y configuración IP.....	26
Tabla 3. Direcciones IP para el SVI.	30

LISTA DE FIGURAS

	Pág.
Figura 1. Escenario 1	10
Figura 2. Verificación BGP AS1	12
Figura 3. Verificación BGP AB2	13
Figura 4. Verificación BGP AS3	15
Figura 5. Verificación BGP AS4	17
Figura 6. Topología escenario 2	18
Figura 7. Verificación vtp SW-AA	20
Figura 8. Verificación vtp SW-BB	20
Figura 9. Verificación vtp SW-CC	21
Figura 10. Verificación enlace troncal en SW-AA	22
Figura 11. Verificación enlace troncal en SW-BB	22
Figura 12. Verificación enlace troncal en SW-AA	23
Figura 13. Verificación de la creación VLAN en SW-BB	25
Figura 14. Ping de verificación en PC1	32
Figura 15. Ping de verificación en el SW-AA	33
Figura 16. Verificación de ping en SW-AA	34

GLOSARIO

CCNP: (Cisco Certified Network Professional) certificación intermedia de los diferentes cursos entregados por CISCO, tanto Enrutamiento (ROUTE) como en Conmutación (SWITCH).

Cisco Packet Tracer: Software de simulación de redes de alto grado de complejidad que permite la práctica y desarrollo de redes como si se estuviera configurando dispositivos reales, este software ofrece simulación, visualización, creación, evaluación.

DHCP: es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres.

Smart Lab: es un centro especializado en difusión de conocimiento, intercambio de experiencias y espacios compartidos de trabajo vinculado a las ciudades inteligentes.

Enrutamiento: Se refiere al proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas.

RESUMEN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The selected evaluation "Practical skills test" is part of the evaluative activities of the CCNP Deepening Diploma, and seeks to identify the degree of development of competencies and skills that were acquired throughout the diploma. The essential thing is to test the levels of understanding and solving problems related to various aspects of Networking.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

En la actualidad las Telecomunicaciones y sistemas han evolucionado a tan altos estándares de seguridad, complejidad y especificaciones técnicas tanto de protocolos de seguridad como de especificaciones técnicas en los diferentes equipos que conforman las redes a nivel mundial por lo cual se ha creado la necesidad de generar cada día más protocolos, estándares, configuraciones que nos permitan brindar servicios oportunos, adecuados, seguros, confiables y de fácil configuración y administración es así que en el presente informe se realizara la solución de diferentes tipos de configuraciones que se realizan en los entornos reales de las redes de comunicación esto con el fin de evaluar y poner en práctica los conocimientos adquiridos en el diplomado.

Para esta actividad, el estudiante debe realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

DESARROLLO DE LA GUIA

Escenario 1.

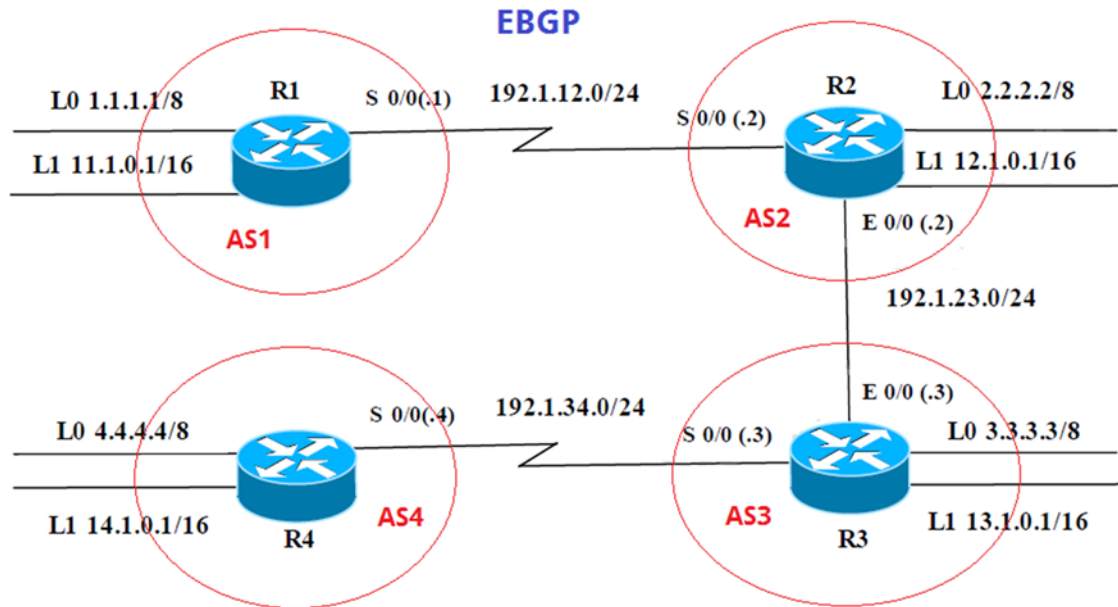


Figura 1. Escenario 1

Información para configuración de los Routers

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0

	Interfaz	Dirección IP	Máscara
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0

R4	Interfaz	Dirección IP	Máscara
	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Tabla 1. Direccionamiento escenario 1

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```

AS1#enable
AS1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AS1(config)#router bgp 1
AS1(config-router)#bgp router-id 22.22.22.22
AS1(config-router)#neighbor 192.1.12.2 remote-as 2
AS1(config-router)#network 1.1.1.1 mask 255.0.0.0
AS1(config-router)#network 11.1.0.1 mask 255.255.0.0
AS1(config-router)#exit
AS1(config)#exit
AS1#
%SYS-5-CONFIG_I: Configured from console by console

AS1#

```

```

AS1#show ip bgp
BGP table version is 4, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0/8        0.0.0.0              0         0 32768 i
*                   192.1.12.2          0         0         0 2 i
*> 11.1.0.0/16      0.0.0.0              0         0 32768 i

AS1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
C      11.1.0.0 is directly connected, Loopback1
C    192.1.12.0/24 is directly connected, Serial0/0/0

AS1#

```

Figura 2. Verificación BGP AS1

```

AS2>enable
AS2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AS2(config)#router bgp 2
AS2(config-router)#bgp router-id 33.33.33.33
AS2(config-router)#neighbor 192.1.12.1 remote-as 1
AS2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

AS2(config-router)#neighbor 192.1.34.3 remote-as 3
AS2(config-router)#neighbor 192.1.23.3 remote-as 3
AS2(config-router)#network 1.1.1.0
AS2(config-router)#network 11.1.0.0
AS2(config-router)#exit
AS2(config)#exit
AS2#
%SYS-5-CONFIG_I: Configured from console by console
AS2#

```

```

AS2#show ip bgp
BGP table version is 6, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 1.0.0.0/8         192.1.12.1             0         0       0 1 i
*> 2.0.0.0/8         0.0.0.0                0         0       0 2 i
*> 3.0.0.0/8         192.1.23.3             0         0       0 3 i
*> 11.1.0.0/16       192.1.12.1             0         0       0 1 i
*> 13.1.0.0/16       192.1.23.3             0         0       0 3 i

AS2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:00:00
C    192.1.12.0/24 is directly connected, Serial0/0/0
C    192.1.23.0/24 is directly connected, FastEthernet0/0

AS2#

```

Figura 3. Verificación BGP AB2

- Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
AS3>enable
AS3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AS3(config)#router bgp 3
AS3(config-router)#bgp router-id 44.44.44.44
AS3(config-router)#neighbor 192.1.12.2 remote-as 2
AS3(config-router)#neighbor 192.1.23.2 remote-as 2
AS3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up

AS3(config-router)#neighbor 192.1.34.4 remote-as 4
AS3(config-router)#network 4.4.4.4 mask 255.0.0.0
AS3(config-router)#network 14.1.0.1 mask 255.255.0.0
AS3(config-router)#network 2.2.2.2 mask 255.0.0.0
AS3(config-router)#network 12.1.0.1 mask 255.255.0.0
AS3(config-router)#network 3.3.3.3 mask 255.0.0.0
AS3(config-router)#network 13.1.0.1 mask 255.255.0.0
AS3(config-router)#exit
AS3(config)#exit
AS3#
%SYS-5-CONFIG_I: Configured from console by console
AS3#
```

```

AS3#show ip bgp
BGP table version is 12, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop              Metric LocPrf Weight Path
*> 1.0.0.0/8               192.1.23.2                0         0      0 2 i
*> 3.0.0.0/8               0.0.0.0                   0         0 32768 i
*                          192.1.34.4                0         0      0 4 i
*> 4.0.0.0/8               192.1.34.4                0         0      0 4 i
*>                          0.0.0.0                   0         0      0 3 i
* 11.1.0.0/16             192.1.23.2                0         0      0 2 1 i
*>                          192.1.34.4                0         0      0 4 i
*> 13.1.0.0/16            0.0.0.0                   0         0 32768 i
*                          192.1.34.4                0         0      0 4 i
*> 14.1.0.0/16            192.1.34.4                0         0      0 4 i
*>                          0.0.0.0                   0         0      0 3 i

AS3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
    11.0.0.0/16 is subnetted, 1 subnets
B      11.1.0.0 [20/0] via 192.1.34.4, 00:00:00
    13.0.0.0/16 is subnetted, 1 subnets
C      13.1.0.0 is directly connected, Loopback1
    14.0.0.0/16 is subnetted, 1 subnets
B      14.1.0.0 [20/0] via 192.1.34.4, 00:00:00
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial0/0/0

AS3#

```

Figura 4. Verificación BGP AS3

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la

Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
AS4>enable
AS4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AS4(config)#router bgp 4
AS4(config-router)#bgp router-id 66.66.66.66
AS4(config-router)#neighbor 192.1.34.3 remote-as 3
AS4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

```
AS4(config-router)#neighbor 192.1.23.3 remote-as 3
AS4(config-router)#neighbor 192.1.23.2 remote-as 2
AS4(config-router)#neighbor 192.1.12.2 remote-as 2
AS4(config-router)#neighbor 192.1.12.1 remote-as 1
AS4(config-router)#network 3.3.3.3 mask 255.0.0.0
AS4(config-router)#network 13.1.0.1 mask 255.255.0.0
AS4(config-router)#network 12.1.0.1 mask 255.255.0.0
AS4(config-router)#network 2.2.2.2 mask 255.0.0.0
AS4(config-router)#network 11.1.0.1 mask 255.255.0.0
AS4(config-router)#network 4.4.4.4 mask 255.0.0.0
AS4(config-router)#network 14.1.0.1 mask 255.255.0.0
AS4(config-router)#exit
AS4(config)#exit
AS4#
%SYS-5-CONFIG_I: Configured from console by console
```

```
AS4#
```



```

AS4#show ip bgp
BGP table version is 12, local router ID is 66.66.66.66
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0/8         192.1.34.3              0      0      0 3 2 i
*> 3.0.0.0/8         192.1.34.3              0      0      0 3 i
*>                   0.0.0.0                0      0      0 4 i
*> 4.0.0.0/8         0.0.0.0                0      0 32768 i
*                   192.1.34.3              0      0      0 3 i
*> 11.1.0.0/16        192.1.34.3              0      0      0 3 2 1 i
*>                   0.0.0.0                0      0      0 4 i
*> 13.1.0.0/16        192.1.34.3              0      0      0 3 i
*>                   0.0.0.0                0      0      0 4 i
*> 14.1.0.0/16        0.0.0.0                0      0 32768 i
*                   192.1.34.3              0      0      0 3 i

AS4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
C    4.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
C    192.1.34.0/24 is directly connected, Serial0/0/0

AS4#

```

Figura 5. Verificación BGP AS4

Escenario 2

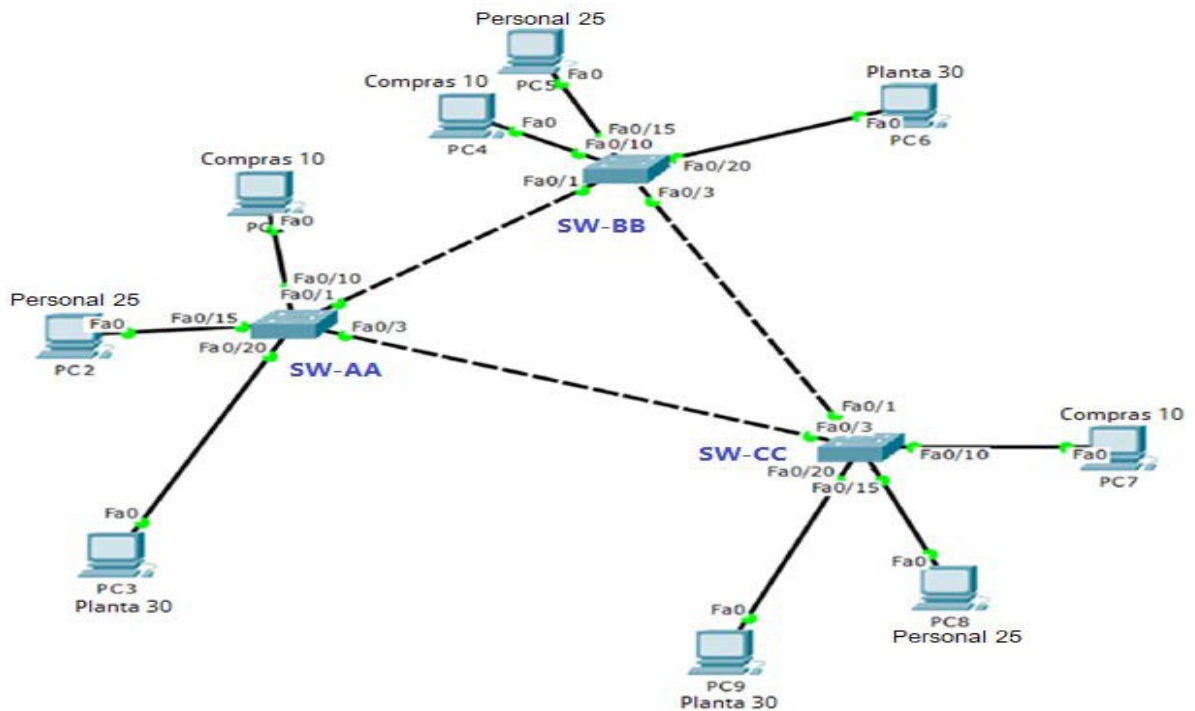


Figura 6. Topología escenario 2

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp version 2
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
```

2. Verifique las configuraciones mediante el comando ***show vtp status***.

```

SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
SW-AA(config)#end
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Client
VTP Domain Name             : CCNP
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x3A 0x49 0xE7 0xED 0x58 0x28 0x41
0x35
Configuration last modified by 0.0.0.0 at 3-1-93 01:21:59
SW-AA#

```

Figura 7. Verificación vtp SW-AA

```

SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
SW-BB(config)#end
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : CCNP
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x56 0x78 0x3B 0x23 0xDA 0x02 0x85
0x84
Configuration last modified by 0.0.0.0 at 3-1-93 01:24:35
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#

```

Figura 8. Verificación vtp SW-BB

```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#
SW-CC(config)#end
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Client
VTP Domain Name             : CCNP
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled

```

Figura 9. Verificación vtp SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es **dynamic auto**, solo un lado del enlace debe configurarse como **dynamic desirable**.

SW-AA>enable

SW-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-AA(config)#interface fastEthernet 0/1

SW-AA(config-if)#switchport mode dynamic desirable

SW-AA(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SW-AA(config-if)#

5. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando **show interfaces trunk**.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

SW-AA(config-if)#end
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none

SW-AA#
```

Figura 10. Verificación enlace troncal en SW-AA

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

SW-BB>enable
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

SW-BB#
```

Figura 11. Verificación enlace troncal en SW-BB

- Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW-AA

SW-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-AA(config)#interface fastEthernet 0/3

SW-AA(config-if)#switchport mode trunk

SW-AA(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

SW-AA(config-if)#

- Verifique el enlace "trunk" el comando **show interfaces trunk** en SW-AA.

```
changed state to up
SW-AA(config-if)#end
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     desirable n-802.1q       trunking      1
Fa0/3     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
Fa0/3     1

SW-AA#
```

Figura 12. Verificación enlace troncal en SW-AA

- Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

SW-BB>enable

SW-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-BB(config)#interface fastEthernet 0/3

SW-BB(config-if)#switchport mode trunk

SW-BB(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

SW-BB(config-if)#exit

SW-BB(config)#

SW-CC>enable

SW-CC#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-CC(config)#interface fastEthernet 0/1

SW-CC(config-if)#switchport mode trunk

SW-CC(config-if)#exit

SW-CC(config)#

C. Agregar VLANs y asignar puertos.

9. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99)

En SW-AA

SW-AA>enable

SW-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-AA(config)#vlan 10

VTP VLAN configuration not allowed when device is in CLIENT mode.

SW-AA(config)#

La configuración VLAN no está permitida cuando el dispositivo esta en modo cliente.

En SW-BB

SW-BB>enable

SW-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.


```

SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#

```

10. Verifique que las VLANs han sido agregadas correctamente.

En SW-BB

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Compras	active	
25	Personal	active	
30	Planta	active	
99	Admon	active	
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trnet-default	active	

Figura 13. Verificación de la creación VLAN en SW-BB

11. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN	190.108.20.X / 24

	25	
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

Tabla 2. Asociacion de los puertos a las vlan y configuración IP.

En SW-AA

```
SW-AA>enable
```

```
SW-AA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
SW-AA(config)#interface vlan 10
```

```
SW-AA(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan10, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

```
SW-AA(config-if)#ip address 190.108.10.1 255.255.255.0
```

```
SW-AA(config-if)#exit
```

```
SW-AA(config)#interface vlan 25
```

```
SW-AA(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan25, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up
```

```
SW-AA(config-if)#ip address 190.108.20.1 255.255.255.0
```

```
SW-AA(config-if)#exit
```

```
SW-AA(config)#SW-AA(config)#interface vlan 30
```

```
SW-AA(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan30, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
```

```
SW-AA(config-if)#ip address 190.108.30.1 255.255.255.0
```

```
SW-AA(config-if)#exit
```

```
SW-AA(config)#
```

En SW-BB

```
SW-BB>enable
```

SW-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-BB(config)#interface vlan 10

SW-BB(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

SW-BB(config-if)#ip address 190.108.10.2 255.255.255.0

SW-BB(config-if)#exit

SW-BB(config)#interface vlan 25

SW-BB(config-if)#

%LINK-5-CHANGED: Interface Vlan25, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up

SW-BB(config-if)#ip address 190.108.20.2 255.255.255.0

SW-BB(config-if)#exit

SW-BB(config)#interface vlan 30

SW-BB(config-if)#

%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

SW-BB(config-if)#ip address 190.108.30.2 255.255.255.0

SW-BB(config-if)#exit

SW-BB(config)#

En SW-CC

SW-CC>enable

SW-CC#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW-CC(config)#interface vlan 10

SW-CC(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

SW-CC(config-if)#ip address 190.108.10.3 255.255.255.0

SW-CC(config-if)#exit

```
SW-CC(config)#interface vlan 25
```

```
SW-CC(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan25, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up
```

```
SW-CC(config-if)#ip address 190.108.20.3 255.255.255.0
```

```
SW-CC(config-if)#exit
```

```
SW-CC(config)#interface vlan 30
```

```
SW-CC(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan30, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
```

```
SW-CC(config-if)#ip address 190.108.30.3 255.255.255.0
```

```
SW-CC(config-if)#exit
```

12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

En SW-AA

```
SW-AA>enable
```

```
SW-AA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW-AA(config)#interface fastEthernet 0/10
```

```
SW-AA(config-if)#switchport mode access
```

```
SW-AA(config-if)#switchport access vlan 10
```

```
SW-AA(config-if)#exit
```

```
SW-AA(config)#
```

En SW-BB

```
SW-BB>enable
```

```
SW-BB#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW-BB(config)#interface fastEthernet 0/10
```

```
SW-BB(config-if)#switchport mode access
```

```
SW-BB(config-if)#switchport access vlan 10
```

```
SW-BB(config-if)#exit
```

```
SW-BB(config)#
```

En SW-CC

```
SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#
```

13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

En SW-AA

```
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
SW-AA(config)#
```

En SW-BB

```
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
SW-BB(config)#
```

En SW-CC

```
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/20
```

```
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
SW-CC(config)#
```

D. Configurar las direcciones IP en los Switches.

14. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 3. Direcciones IP para el SVI.

En SW-AA

```
SW-AA(config)#interface vlan 99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#
```

En SW-BB

```
SW-BB(config)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SW-BB(config-if)#exit
SW-BB(config)#
```

En SW-CC

```
SW-CC(config)#interface vlan 99
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

```
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#
```

E. Verificar la conectividad Extremo a Extremo

15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

El ping entre cada una de las PC es correcto solo si hacen parte de la misma Vlan, de lo contrario el ping es incorrecto

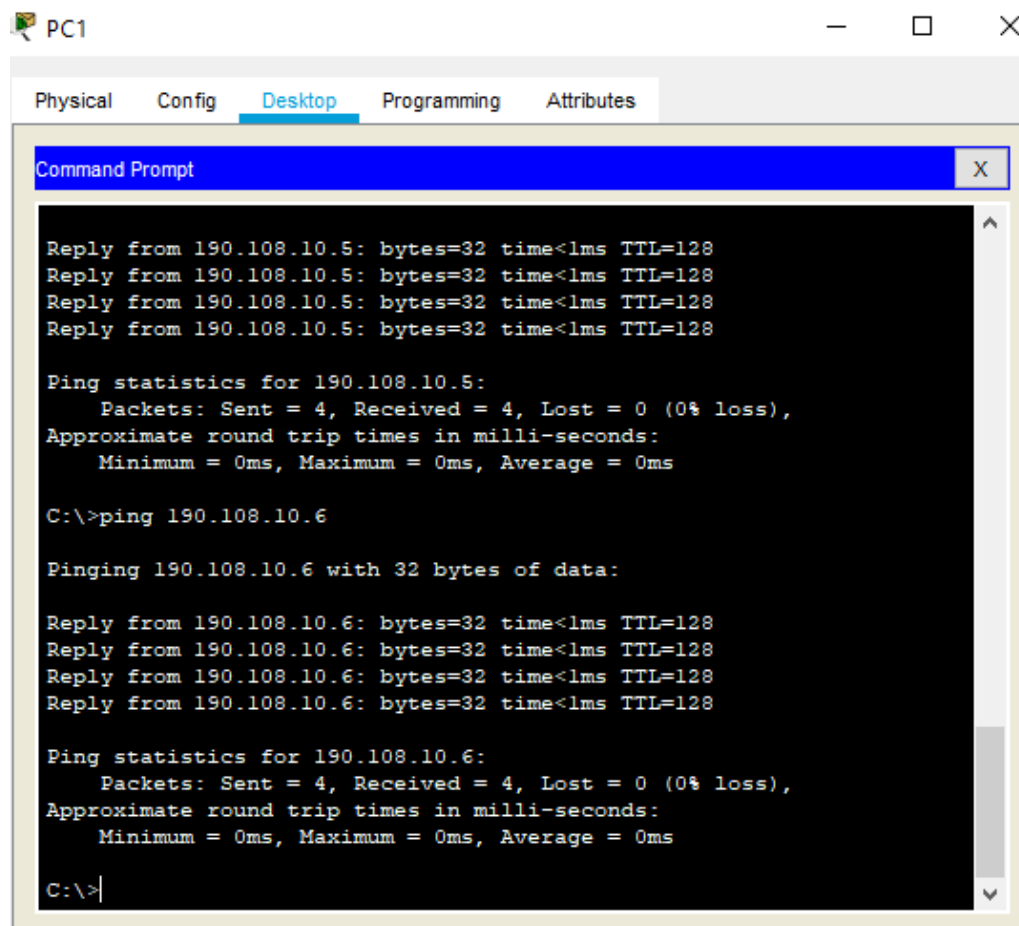


Figura 14. Ping de verificación en PC1.

16. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Al ejecutar un ping de cada ping a los demás, el resultado es exitoso, debido a que se reconoce el direccionamiento de la Vlan 99, entonces, al realizar un ping desde un switch a la Vlan 99 de otro switch, el pingo es exitoso.


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#
```

Figura 15. Ping de verificación en el SW-AA

17. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

El ping es correcto dado a que los switches reconocen los direccionamientos de las vlan asociadas y de esta forma se encarga de redirigir el enrutamiento a los equipos conectados dentro de su red.

SW-AA

Physical Config CLI Attributes

IOS Command Line Interface

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

SW-AA#ping 190.108.20.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#ping 190.108.30.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#ping 190.108.30.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#
```

Figura 16. Verificación de ping en SW-AA

CONCLUSIONES

Se logró demostrar la capacidad para configurar y administrar dispositivos de Networking en diseños de redes escalables y de conmutación, a través de los conocimientos adquiridos durante el curso de profundización, para establecer niveles de seguridad básicos en una red.

CCNP se ha diseñado para reflejar las habilidades y las responsabilidades laborales asociadas a los roles profesionales de ingeniero de redes, ingeniero de sistemas, ingeniero de soporte de redes, administrador de redes, asesor de redes e integrador de sistemas Ingeniero de telecomunicaciones y demás profesiones afines.

El desarrollo de este trabajo permite reforzar los demás conocimientos adquiridos a través de la realización de los laboratorios durante el transcurso activo del curso y la solución de las lecciones evaluativas en el entorno de cisco (Netacad).

REFERENCIAS BIBLIOGRÁFICAS

Froom, R., Frahim, E. (2015). CISCO Press (Ed). High Availability. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>
<https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2>
<https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning

Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Enterprise Internet Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInMfy2rhPZHwEoWx>